User's Manual & Installation Guide for: WiN52XX/WiN51XX Series Outdoor CPE

ALL RIGHTS RESERVED

Disclaimer Of Liability

We have checked the contents of this manual against the hardware and software described. However, deviations from the description cannot be completely ruled out.
RuggedCom shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.
The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RuggedMAX-BST™, RuggedServer™, RuggedWireless™, RuggedCom Discovery Protocol™ (RCDP™), RuggedExplorer™, Enhanced Rapid Scanning Tree Protocol™ (eRSTP™), are trademarks of RuggedCom Inc. Rugged Operating System® (ROS®) and RuggedSwitch® are registered trademarks of RuggedCom Inc. Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Warranty

Five (5) years from date of purchase, return to factory. For warranty details, visit www.ruggedcom.com or contact your customer service representative.

Contacting RuggedCom

Corporate Headquarters	US Headquarters	Europe Headquarters
RuggedCom Inc	RuggedCom	RuggedCom
30 Whitmore Road	1930 Harrison St., Suite 209	Unit 41, Aztec Centre,
Woodbridge, Ontario	Hollywood, Florida	Aztec West, Almondsbury, Bristol
Canada, L4L 7Z4	USA, 33020	United Kingdom BS32 4TD
Tel: (905) 856-5288	Tel: (954) 922-7938x103	Tel: +44 1454 203 404
Fax: (905) 856-1995	Fax: (954) 922-7984	Fax: +44 1454 203 404
Toll-free: 1 (888) 264-0006	Toll-free: 1 (888) 264-0006	Toll-free: 1 (888) 264-0006
Email: RuggedSales@RuggedCom.com		

Table of Contents

1

ntroduction

1.1 About this Manual

This manual describes the installation procedures of WiN51XX/WiN52XX Outdoor CPE with Ethernet interface and is written for the installers and operators.

WiN51XX/WiN52XX 2 products will be referred in this manual as WiN5200 from now on.

The RuggedCom WiN5200 is a member of the Win-Max™ E family, a line of mobile WiMAX broadband wireless access systems based on the 802.16e mobile WiMAX standard. The Win-Max™ E family is detailed in the System Description manual of RuggedCom.

This manual assumes that users have some experience with WiMAX technologies and procedures.

While some safety precautions are reviewed here, this manual assumes that installers have been trained in safe installation practices. Users, who are new to WiMAX technologies and service procedures, should not rely on this manual for comprehensive guidance.

1.2 General Description

The RuggedCom WiN5200 ODU is a member of the Win-Max™ E family, a line of WiMAX Broadband Wireless Access systems based on the 802.16e mobile WiMAX standard, specially designed for quadruple-play applications.

WiN5200 is a high-performance outdoor unit that provides complete 802.16e mobile WiMAX broadband wireless access functionality to a range of indoor multi-service gateways.

The WiN5200 enables the full scope of triple-play (including telephony, data, Video-on-Demand) over the WiMAX network. In the home, triple play services are distributed to a single gateway for a simple home-networking solution.

The WiN5200 is based on the IEEE 802.16e standards to effectively meet the unique requirements of the wireless Metropolitan Area Network (MAN) environment and to deliver broadband access services to a wide range of customers. Specifically designed for point-to-multipoint broadband wireless access applications, the WiN5200 provides efficient use of the wireless spectrum, supporting a range of user environments. The access and bandwidth allocation mechanisms accommodate hundreds of subscriber units per sector, supporting differentiated services to a multiple of end-users.

1.2.1 Features

- Intelligent WiMAX subscriber unit for wireless triple-play service delivery
- Outdoor unit with ETH interface to indoor unit
- Automatic, self-configured, plug-n-play
- Supporting 1.X, 2.X and 3.X GHz bands

1.3 Package Components and Unpacking

Check that the package contains:

1. WiN52xx ODU with integrated flat antenna
2. Pole/wall mounting hardware

In case of damage, contact the shipping company.

1.4 Safety Information

RF Exposure

The WiN5200, an outdoor CPE, is compliant with the requirements set forth in CFR 47 section 1.1307, addressing RF Exposure from radio frequency devices as defined in OET Bulletin 65. The outdoor CPE mobile unit should be positioned more than 0.6 feet (20 cm) from humans. The outdoor CPE fixed unit should be positioned at least 7 feet (2m) from humans.

Lightning Protection

When WiN5200 is installed in an outdoor location, all indoor components (Ethernet, power supply) should be connected through a lightning protector.

The purpose of the lightning protection is to protect people and equipment located indoors from lightning that might strike the WiN5200 or its outdoor cables. Therefore, the lightning protector device should be installed indoors, as close as possible to the point where the cables enter the building. The lightning protector can also be installed outdoors, as long as the cables that lead from it indoors are well protected from lightning between the box and the building entrance.

Power Cord Protection

The WiN5200 should always be connected to the WiN1010 data adapter for both power supply and data transfer purposes.

Any other type of connection/application of the WiN5200 and/or WiN1010 is not allowed.

Route all power supply cords so that people cannot walk on them, or place objects on or against them. This can pinch or damage the cords.

Servicing

Do not open the cover of this product and perform corrective actions unless instructed to do so in the operating instructions.

Outdoor Grounding System

Verify that the antenna or cable system is grounded (earthed).

The antenna is an integral part of the CPE (Models WiN51XX)

The CPE (antenna) installation must be as per Article 810 of the NEC. Of particular note is the requirement that the grounding conductor not be less than 10 AWG (Cu). The scheme should be either in accordance with UL 96 and 96A. Lightning Protection Components and Installation Requirements for Lightning Protection Systems, or tested in accordance with UL 50 and UL 497.

CAUTION

To reduce the risk of fire, use only No. 26AWG or larger telecommunication line cord between the indoor and outdoor units.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:

(1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device

Changes or modifications to this equipment not expressly approved by the party responsible for compliance (RuggedCom Inc.) could void the user's authority to operate the equipment.

2

roduct Description

2.1 Introduction

The WiN5200 ODU CPE is an IEEE 802.16-2005 compliant wireless device for deployment of point-to-multipoint (PMP) and point-to-point (PTP) network architectures.

The WiN5200 ODU CPE is an outdoor device. The WiN5200 ODU CPE is WiMAX Forum 802.16e Wave 2 (MIMO) Certified subscribers. Each subscriber registers and establishes a bi-directional data link with the base station sector controller.

The CPE terminals are grouped into two classes, Outdoor CPEs and Residential Gateways (RG) which are indoor units. The relationship between all the units is illustrated below.

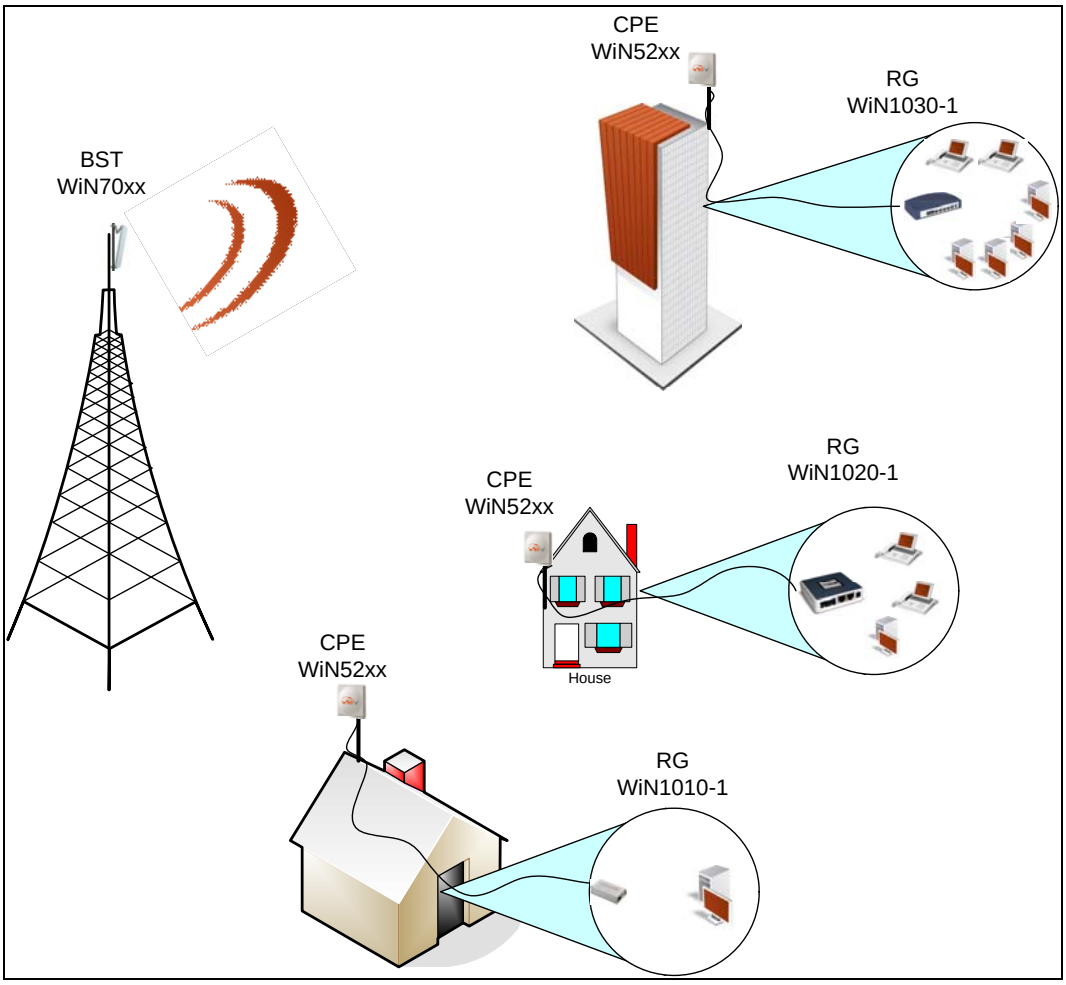


Figure 2-1: Functional Overview of the CPEs

The base station is connected to the head-end over IP Backhaul or via wireless channels. The outdoor CPEs are connected to the base station over wireless channels. The outdoor CPE is connected to the indoor residential gateway over Ethernet or coaxial networks.

2.2 IEEE 802.16e Mobile WiMAX Compliance

The IEEE 802.16-2005 specifications describe a PMP broadband wireless access standard for systems. This standard includes descriptions for both the Media Access Control (MAC) and the physical (PHY) layers.

The WiN5200 ODU CPE is compliant to IEEE 802.16-2005 WiMAX forum Wave 2 profile.

Note

The 802.16e standards are subject to amendment, and Win-MaxTM product family design compliance applies to a specific revision of the standard. The Win-MaxTM product family does not support mesh communication (direct subscriber-to-subscriber).

2.3 Block Diagram

The CPE consists of the following modules:

1. Base-Band board – including the WiMAX 16e MIMO Base-Band SoC (running the 16e MAC + PHY) plus the User Interface plus the analog front end that interface the RF module.
2. Power Supply board– DC/DC power supply. Converts the 48VDC to the various voltages that are feeding the Digital and the RF modules
3. RF board - Single transmit dual receive module that modulate the analog WiMAX signal input from the Base-Band modem to the high frequency RF output. Several RF modules exist - each supporting different frequency band.
4. Chassis
5. Antenna – Integrated dual polarization antenna to support the MIMO schemes

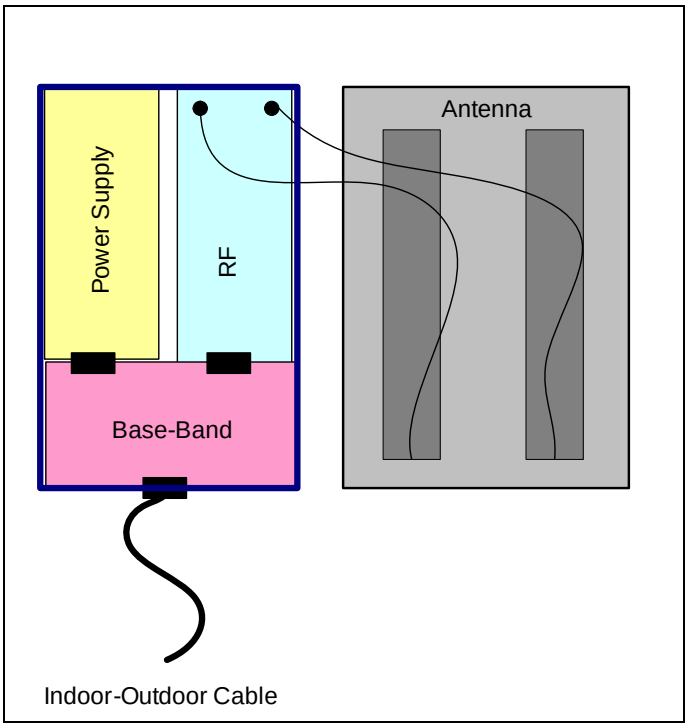


Figure 2-2: WiN5200 Block Diagram

2.4 Features

2.4.1 Mobile WiMAX Wave 2 MIMO Features

Multiple-Input, Multiple-Output (MIMO) describes systems that use more than one radio and antenna system at each end of the wireless link. In the past it was too costly to incorporate multiple antennas and radios in a subscriber terminal. Recent advances in radio miniaturization and integration technology now makes it feasible and cost effective. Combining two or more received signals has the immediate benefit of improving received signal strength, but MIMO also enables transmission of parallel data streams or greater throughput. For example, in a 2 x 2 MIMO (two transmit and two receive elements), dual polarization point-to-point system, the carrier's allocated frequency can be used twice, effectively doubling the throughput data rate.

In point-to-multipoint systems employing MIMO, each base station antenna transmits a different data stream and each subscriber terminal receives various components of the transmitted signals with each of its subscriber antennas as illustrated in the figure below. By

using appropriate algorithms, the subscriber terminal is able to separate and decode the parallel simultaneously received data streams.

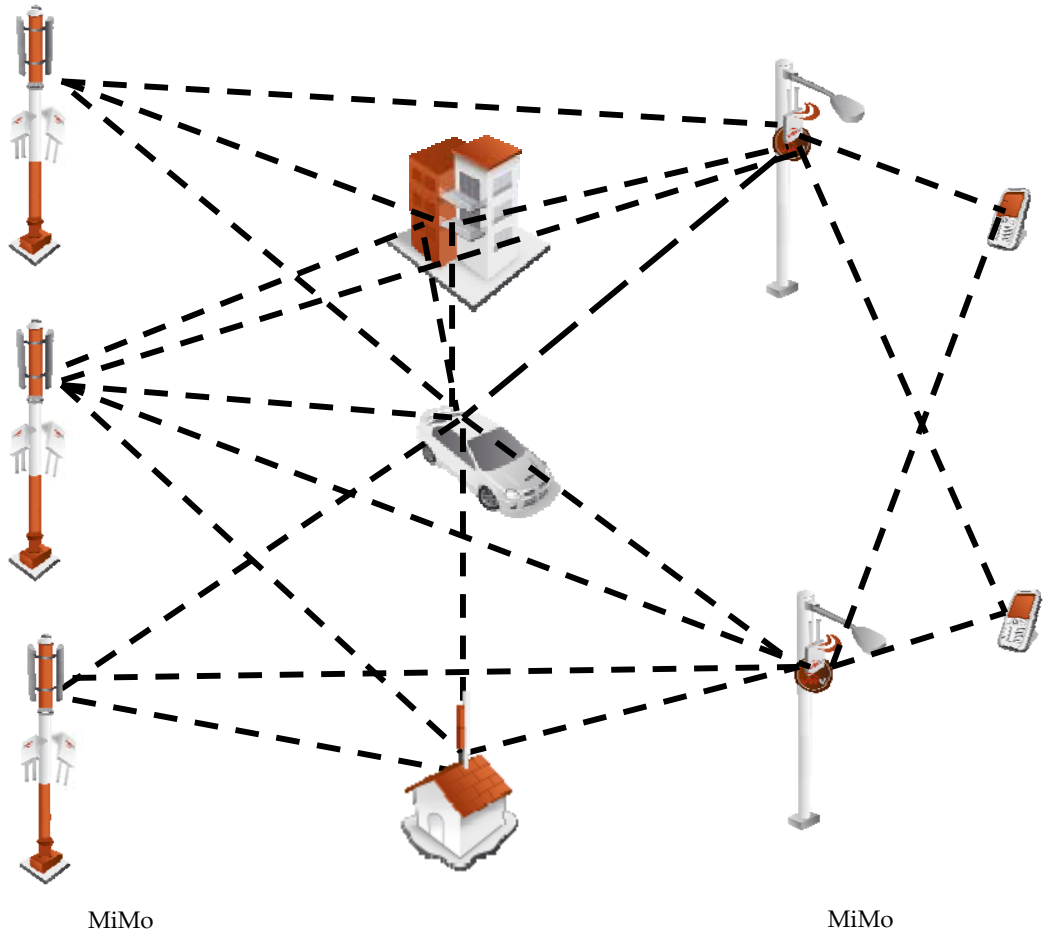


Figure 2-3: MiMo Antenna System

2.4.1.1 Space-Time Coding

Space-time coding (STC) is a technique for implementing transmission diversity. Mobile WiMAX uses transmit diversity in the downlink direction to provide spatial diversity that enhances the signal quality to a specific subscriber located anywhere within the range of the antenna beam. Although providing less signal gain than beam-forming, transmit diversity is more robust for mobile users since it does not require prior knowledge of the path

characteristics of a subscriber's particular frequency channel. One such STC technique, known as the Alamouti Code, was published in 1998[4] and has been incorporated into the WiMAX 16e standard.

2.4.2 Security

Security was a key failing of older broadband wireless systems of the past. The why of it is easy to comprehend---any network that transmits its data across wireless signals rather than wires is inherently more open to interference, intrusion or assault. This does not mean solid broadband wireless security is impossible, just much more difficult.

As broadband wireless networks have matured security features have improved. With the advent of WiMAX, the security toolsets available to broadband wireless service providers have reached all time highs of functionality. Today's WiMAX networks can be secured more effectively than ever before.

WiMAX and IEEE 802.16 Security Sub layer provides for privacy, authentication and confidentiality across the broadband wireless network. Defined initially by IEEE 802.16-2004 and then corrected and amended by Corrigendum 1 and IEEE 802.16e-2005 respectively, the Security Sub layer now supports Fixed and Mobile operation.

There are two major differences between the standards. The first difference is that the security mechanism of the IEEE 802.16-2004 is based on the DOCSIS standard. In the 802.16e-2005 many changes have been made in the security mechanisms. The second difference is in the flexibility of SS's connection characteristics with the BST. The IEEE 802.16-2004 only supports fixed access. In fixed access, an SS cannot mitigate to the air interface of a new Base Station (BST) without performing the network entry again after a connection termination. The IEEE 802.16e-2005 supports mobile access. Mobile access enables an SS to move between various BST cells while keeping the connection established.

There are five primary aspects of WiMAX security that should be considered when designing a security plan for a WiMAX network. These range from mitigation techniques at the physical layer to improved wireless authentication and encryption to intrusion protection and data transport security. At each level, choices in implementation and security levels can be made; although in the case of the physical layer options are limited.

2.4.2.1 Physical Layer Security

There are two basic types of attacks that can affect the physical layer of WiMAX. One is jamming and the other is packet scrambling. The first is relatively straightforward, and is sometimes the result of interference rather than an attack. Jamming consists of a stronger

signal than the WiMAX network overwhelming network data feeds either in intermittent bursts or with sustained carrier waves.

Since most WiMAX network services are delivered over licensed bands (currently 3.5 GHz internationally and 2.5 GHz both internationally and in the US), this offers spectrum relatively quiet from accidental interference. Accidental interference in licensed spectrum cannot always be completely discounted as there is a possibility of second and third harmonic interference waves, for example, from much lower frequency signals if those are in close proximity to the WiMAX antenna systems or that cross them with a signal close enough in physical proximity to locally overload the WiMAX signal. In practice, this is rare.

Packet scrambling is an attack that occurs when control packets in the respective downlink and uplink subframes are sniffed then scrambled and returned to the network. This attack is much harder to mount than a jamming attack. Since most WiMAX networks today use time division duplexing (TDD), to include the Win-Max™ system, an attacker can parse this timing sequence and capture control data, the preamble and map, scramble them and send them back with correct timing to interrupt legitimate signal, resulting in slowdowns and effectively lowered bandwidth. Intercepted and scrambled packets are possible with frequency division duplexing (FDD) as well which transmits both the uplink and downlink simultaneously, but it is even harder to exploit this attack than with TDD systems.

While it may seem the physical layer is inherently most vulnerable as the security elements of WiMAX are located at higher layers, the fact is hackers can often find lower hanging fruit in terms of useful exploits higher in the stack, because as WiMAX supports multiple selections on what service providers can choose to implement in terms of authentication, sometimes the door can be left open for them by the choices made.

2.4.2.2 Authentication

Traditionally the first level of security authentication for older broadband wireless technologies has been MAC authentication and WiMAX supports this, although providers don't settle for this method. This technique allowed service providers to log permitted MAC device addresses and allow only those addresses to access the network. Hackers long ago figured out how to spoof these. If a base station is not set up with adequate authentication measures, an attacker can capture control packets and pose as a legitimate subscriber even with older MAC device authentication enabled.

A second, newer and much better choice, embraced by the Win-Max™ system, is the built in support for X.509 device certificates embedded with the use of extensible authentication protocol---transport layer security (EAP-TTLS) method, added with the 802.16e standard and WiMAX Forum.

Enter the EAP-TLTS authentication method. This technique allows both the subscriber and the base station to authenticate each other using an X.509 method for both, in addition to a subscriber authentication which is based on well-known subscriber authentication techniques such PAP and MS-CHAP. MAC control headers are never encrypted in WiMAX, however with EAP carriers can choose to authenticate them (but they don't necessarily have to). This capability adds an additional layer of authentication confirmation. It's an operator specific guideline decision and is tunable in the Win-Max™ system.

2.4.2.3 Encryption

Clearly the first layer of defense for WiMAX operators is to authenticate a legitimate user on its network. However, WiMAX, with its 802.16e ratification, offers top line tools for encryption of data. Older wireless iterations used the data encryption standard (DES) which relied on a 56-bit key for encryption. This is largely considered obsolete. WiMAX 802.16e certainly supports DES (3DES) but it also adds support for the Advanced Encryption Standard (AES) which supports, 128-bit, 192-bit or 256-bit encryption keys. Also AES meets the Federal Information Processing Standard (FIPS) 140-2 specification, required by numerous governmental branches. This technology, which requires dedicated processors on board base stations, is robust and highly effective.

Traffic encryption may be employed per 802.16 Service Flow and is subject to operator policy.

The relevance of encryption to the network operator deployment is questionable. In the past, for example, many cellular carriers focused on authentication and mostly ignored encryption. Whether that will change as mobile service providers ramp up more broadband applications is an open question.

The downside to these heavy computing tasks (i.e. authentication and encryption) is that all of this requires processor cycles, which may affect the performance of the system. Nevertheless, the Win-Max™ system and especially, the SS and BST, which are the entities that take active role in heavy security-related computations, were built bottom to top with a design goal of offloading heavily computing tasks from the host processor to a specific circuit. Consequently, no performance degradation is neglected.

2.4.2.4 Third Party Intrusion Protection

We examined WiMAX authentication schemes, which are a major component of a secure network. And we also spoke of data encryption. Clearly, WiMAX possesses solid tools already built in. But there are considerations beyond just good security that can drive a migration to third party intrusion detection and protection tools---namely business case elements. Intrusion protection is however, not data protection. These are two different classes of solution. Certainly, a good third party intrusion protection can monitor and secure a network's authentication. However, many solutions also offer worm protection, Trojan horse

protection, defenses against viruses, backdoor exploits and denial of service attacks to name a few. Some of these elements are almost a business necessity for a wireless service provider and may justify the cost of an additional security suite initially. For other companies, a migration strategy to enhanced tools makes the most cost effective sense.

A good place to start is examining market and service scenarios. If your customer base is highly sensitive to data integrity (financial sector or hospital customers) third party intrusion prevention systems can help segment customers from each other better as well as secure them from outside attack.

Or in another example, a mobile network that offers just Internet access and voice may wish to abrogate responsibility for data encryption and use session initiation protocol (SIP) signaling for its VoIP and WiMAX native authentication tools.

Referring to encryption, clearly an AES supported data encryption system gives WiMAX excellent security in this regard. However, additional solutions that meet customer needs such as virtual private networks may enhance the business model and provide additional source of revenue.

2.4.3 Time Division Duplexing (TDD)

The WiN5200 CPE uses time division duplexing (TDD) to transmit and receive on the same RF channel. This is a non-contention based method for providing an efficient and predictable two-way PTP or PMP cell deployment. All uplink and downlink transmission scheduling is managed by the base station. The base station sends data traffic to subscribers, polls for grant requests, and sends grant acknowledgements based on the total of all traffic to all subscribers.

2.4.4 Coding Rate

Each burst of data transmitted over the wireless interface is padded with redundant information, making it more resistant to potential over-the-air errors. The coding rate is the ratio of user data to the total data transmitted including the redundant error correction data. The base station supports coding rates of 1/2, 2/3, and 3/4.

2.4.5 Modulation

The modulation technique specifies how the data is coded within the OFDMA carriers. The base station supports QPSK, 16 Quadarature Amplitude Modulation (QAM), and 64 QAM modulations.

2.4.6 Convolution Coding Error Correction

Convolution Coding (CC) error correction is enabled for all traffic rates. This low-level process can correct bursts of errors in received messages and reduce the number of retransmissions.

2.5 Deployment Models

The CPE supports point to point (PTP) and point to multipoint (PMP) deployment scenarios.

2.5.1 PTP Deployment

When deployed in a PTP configuration the base station establishes a dedicated bidirectional link to a single subscriber. The PTP deployments typically use a directional narrow beam antenna for both ends of the link.

2.5.2 PMP Deployment

When deployed in a PMP configuration the base station establishes bi-directional links to more than one subscriber. PMP deployments typically use a wide beam (sector) antenna at the base station and a narrow beam antenna at the subscriber. Service flows are used to police service level agreements for each subscriber.

2.5.3 Non Line-of-Sight

The WinMAX product family supports line-of-sight (LOS) and non line-of-sight (NLOS) operation. A clear LOS link has no obstacles within 60% of the first Fresnel zone of the direct path.

A wireless link is considered non-LOS if natural or man-made structures block the visible path between the base station and the subscriber. In this case, a wireless link can be established only if a reflective path can be established between the base station and subscriber.

2.5.4 Channelization

The CPE is a frequency-specific system, with the frequency band defined by the PHY unit. The use of the operating band must be in accordance with local regulation requirements.

The CPE divides the available frequency band into channels. Allocation of channels during deployment is dependent on spectrum availability in the licensed band and local licensing requirements and conditions. Channel selection allows planners to obtain the maximum geographic coverage, while avoiding frequency contention in adjacent sectors.

2.6 Service Flows

Service flows are a key feature of the 802.16e standard.

A Service Flow represents a unidirectional data flow having separate QoS settings for uplink and downlink. Service flows provide the ability to set up multiple connections to each subscriber in a sector.

Separate service flows can be established for uplink and downlink traffic, where each service flow is assigned a unique service level category and separate QoS settings. This feature allows segregation of high-speed/high-priority traffic from less time-critical flows.

2.6.1 Service Flow Classification

Data packets are forwarded based on classification rules. Classification rules require examining each packet for pattern matches such as destination address, source address, IP TOS, or VLAN tag. All classification is defined at the base station and the classification parameters are downloaded to the subscriber.

2.6.2 Dynamic Service Addition

Service flows are defined and stored in the base station. For each service flow to be established, the base station sends a setup message to the subscriber specifying the required set of QoS parameters. The subscriber responds to each request by accepting or rejecting the setup message.

A service flow may be pre-provisioned or can be dynamically created and deleted without service outage. This is useful for supporting multiple subscribers in a single sector. New subscribers can be added and existing subscribers can be removed or have service levels modified.

Setup messages are sent by the base station following any subscriber power-cycle, loss and recovery of the wireless link to a subscriber, or any service flow add/delete operation at the base station.

2.6.3 Default Service Flows

Default UL/DL service flows are created automatically for each registered subscriber.

These service flows are used to pass all traffic not matching any user-defined service flow (such as broadcast ARP) between the base station and subscribers. The default service flow capacity is limited for each subscriber.

2.6.4 Scheduling

The base station enforces QoS settings for each service flow by controlling all uplink and downlink traffic scheduling. This provides non-contention based traffic model with predictable transmission characteristics. By analyzing the total of requests of all subscribers, the base station ensures that uplink and downlink traffic conforms to the current service level agreements (SLAs). Centralized scheduling increases predictability of traffic, eliminates contention, and provides the maximum opportunity for reducing overhead.

A regular period is scheduled for subscribers to register with the base station. These subscribers may be newly commissioned or have been deregistered due to service outage or interference on the wireless interface. This is the only opportunity for multiple subscribers to transmit simultaneously.

Real-Time Polling Service (rt-PS)

The base station schedules a continuous regular series of transmit opportunities for the subscriber to send variable size data packets. The grant size is based on the current data transfer requirement. Typical applications include streaming MPEG video or VOIP with silence suppression. This is efficient for applications that have a real-time component and continuously changing bandwidth requirements.

Extended Real-Time Polling Service (ert-PS)

The base station schedules a continuous series of transmit opportunities for the subscriber to send variable size data packets. This schedule supports real-time applications including VoIP with silence suppression. The dynamically scheduled grants guarantee reserved bandwidth and reduce latency introduced by repetitive grant requests. The service flow will not transmit packets larger than nominal grant interval.

Non-Real-Time Polling Service (nrt-PS)

The base station schedules regular transmit opportunities for the subscriber to send variable size data packets. Typical applications may include high bandwidth FTP. The polling period may typically be one second or less, even during periods of network congestion.

Best Effort (BE)

The base station schedules transmit opportunities for the subscriber to send traffic based on unused bandwidth after all higher level traffic scheduling requirements are serviced.

Typical applications may include Internet access and email. Best effort service flows can be assigned a priority of 0 to 7.

Unsolicited Grant Service (UGS)

The base station schedules a continuous series of transmit opportunities for the subscriber to send fixed size data packets. This schedule supports real-time applications including VoIP or TDM transport. The UGS pre-scheduled grants guarantee reserved bandwidth and reduce latency introduced by repetitive grant requests. The service flow will not transmit packets larger than nominal grant interval.

2.7 Physical Description

The WiN5200 CPE housing holds the electronic modules and the connection panel detailed below.

Figure 2-4: WIN5200 – Top View

Dimensions (HxWxD w/o the antenna): 22cm x 9.2cm x 6cm

Weight: <1.5 Kg

2.7.1 Physical Interfaces Description

The interconnection panel holds the external connectors used to connect the equipment to the network, power supply and antennas as illustrated below. The interconnection panel holds the connectors as listed below.

Table 2-1: External Connectors

Name	Description	Connector Type
ETH + PWR	Data and power from WiN1010	RJ-45
	Grounding screw	

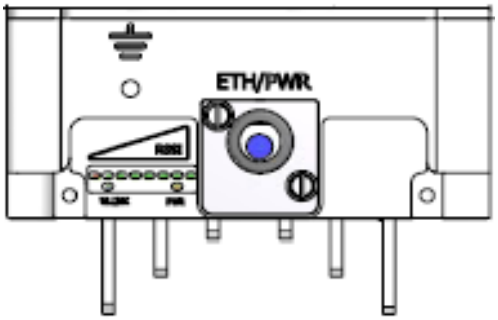


Figure 2-5: Interconnection Panel

2.7.2 LED Indication Description

The LED indications are located on the bottom panel of the outdoor unit. The CPE has the following LED indications:

- LINK QUALITY bar display – display the RSSI level
- WLNK – wireless link indication
- PWR – power ok indication

The LED functionality is described in the table below.

LEDs	Color	Description
WLNK is On	Green	CPE is connected with and receives services from Base station (Network Entry completed)
PWR is on	Green	CPE power is good
One bar LED is On (Least significant)	Green	5dB ≤ SNR < 10dB
Two bar LEDs are On	Green	10dB ≤ SNR < 15dB

Three bar LEDs are On	Green	15dB ≤ SNR < 20dB
Four bar LEDs are On	Green	20dB ≤ SNR < 24dB
Five bar LEDs are On	Green	SNR ≥ 24dB and RSSI < -75dBm
Six bar LEDs are On	Green	SNR ≥ 24dB and RSSI ≥ -75dBm
Seven bar LEDs are On	Green	SNR ≥ 24dB and RSSI ≥ -70dBm
Eight bar LEDs are On	Green	SNR ≥ 24dB and RSSI ≥ -60dBm
Only the 8th LED is On (Most significant)	Green	RSSI ≥ -20dBm (saturation)

3

ounting

3.1 General

The CPE mounting kit, which enables several mounting options such as in the following examples:

1. Poles
2. Walls

When choosing the mounting location for the unit, consider the available mounting structures, antenna clearance.

3.2 Site Survey

Most wireless networks include many CPEs and BSTs installed in various locations in an overlapping radio-cell pattern. It is important to position each CPE at an optimal location and the assignment of its radio channels. Therefore, a site survey becomes an essential first step before physically deploying the RuggedCom solution.

Installation of the CPEs requires a backhaul to interface the corporate network or Internet. This backhaul connection can be an Ethernet-wired connection, a wireless–connection, or a third party solution.

The site survey should include a detailed planning of the WiMAX system deployment. The system deployment plan should include mounting points and the routes for the power and backhaul cables.

Recommended Site Requirements

It is highly recommended that the WiN5200 CPEs be mounted near the edge of the roof of a tall building. The WiN5200 CPEs should be pointed in the direction of the area to be covered. To provide maximum coverage, multiple WiN5200 CPEs can be installed on the same rooftop. However, it is important to leave some distance between each unit in order to prevent interference between the units themselves. When choosing the ideal location, it is also important to take into consideration the overall area topology.

3.3 Pole Mounting

Select a mounting location. You can attach the WiN5200 to any pipe or pole with diameter 1.75″ to 10″.

3.4 Wall Mounting

Select a mounting location. You can attach the WiN5200 to any wall, Outer wall is preferred (typically on a roof or high location to avoid interference from other buildings or trees).

Ensure that the wall mount installation can hold the load of the ODU.

4

nstallation Procedure

4.1 Safety Hazards

	Warning Installing the WiN5200 can pose a serious hazard. Be sure to take precautions to avoid the following: Exposure to high voltage lines during installation Falls when working at heights or with ladders Injuries from dropping tools Contact with AC wiring

4.2 Tools and Cables Required for the Installation

WiN5200 Ethernet ODU CPE Requirements:

IDU-to-ODU Cat5e Ethernet cable (100m MAX) and two RJ-45 plug connectors

Note

The Cat5e Ethernet cable is not included. Please refer to "Appendix B – IDU to ODU cable specification" for detailed technical specifications.

RJ-45 connectors crimping tool

Ground cable with an appropriate termination

General Installation Tools:

Flat Screwdriver
Wrench
Driller
Hammer

Adjustable Ratcheting Socket Wrench

4.3 Installing the WiN5200

The installation involves the WiN5200 and the mounting bracket. The mounting bracket should be installed at the first instance and the WiN5200 should be inserted into it, as detailed in the following instructions.

4.3.1 Pole Mounting

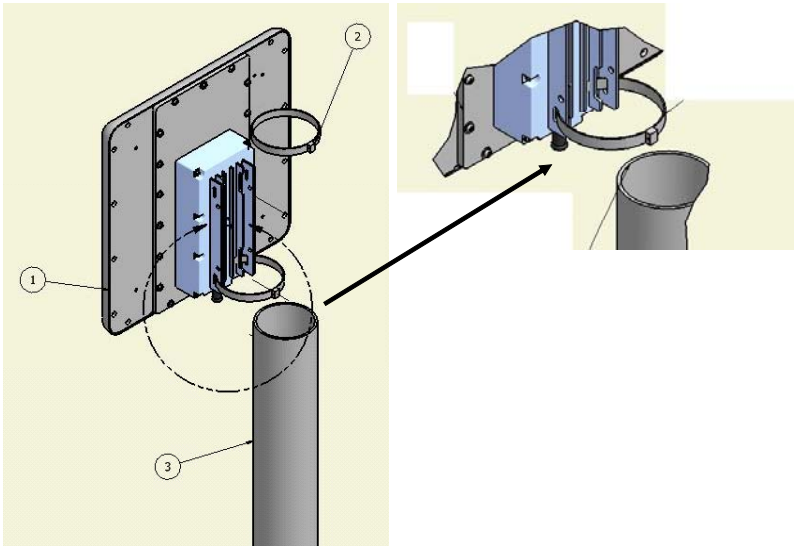


Figure 4-1: Pole Mounting

Follow the steps listed below to install the outdoor device on a pole

1. Select a mounting location on the pole
2. Slide the two adjustable hose clamps along the pole via the holes of the mounting bracket of the outdoor device
3. Adjust the two adjustable hose clamps by the means of a Adjustable Ratcheting Socket Wrench
4. Attach outdoor device using the two adjustable hose clamps to the pole
5. Fasten two adjustable hose clamps by the means of a Adjustable Ratcheting Socket Wrench
6. Fasten the two adjustable hose clamps by the means of a Adjustable Ratcheting Socket Wrench.

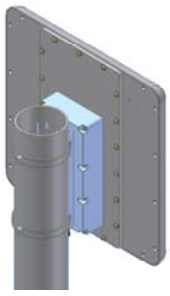
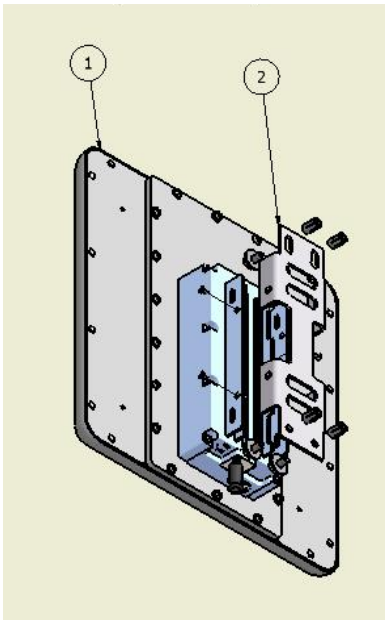
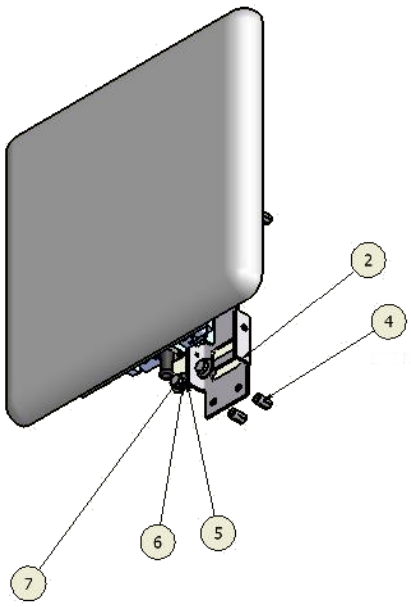


Figure 4-2: WiN5200 Pole Mounted

4.3.2 Wall Mount



Rear View



Front View

Parts List			
ITEM	QTY	PART NUMBER	DESCRIPTION
1	1	AST0003	SU 16e TOP ASSEMBLY
2	1	MPH00453	SU16e WALL MOUNT BRACKET
3	4	MSH12803	SCRW FH 100 DEG 6-32 X3/8
4	4		PHILIPS_FASTENER
5	4	MWH12205	WASHER FLAT NC 1/4
6	4	MWH12210	WASHER SPRING NC 1/4
7	4	MSH12510	SCREW NC1/4X1/2 HEX

Figure 4-3: WiN5200 Wall Mount

Follow the steps listed below to install the WiN5200 on a wall

1. Select a mounting location on the wall
2. Place the wall mounting bracket on the wall and mark 4 holes (2 on the top and 2 on the bottom)
3. Drill 4 holes (2 on the top and 2 on the bottom) for the fastening inserts
4. Insert fastening inserts type NC ¼ into the holes
5. Insert 4 flat washers and 4 spring washers and 4 screws type NS1/4 X ½ HEX (2 on the top and 2 on the down) via the holes on the mounting bracket
6. Attach the wall mounting bracket at this location

7. Press the screws till they match the inserts
8. Fasten the screws with a screwdriver
9. Use flat screwdriver
10. Insert the WiN5200 so that the wall mounting bracket holes match the holes of the mounting bracket of the device
11. Insert four flat washers, four spring washers and four screws (type NC ¼ x ½ HEX) and press until they match the treads of the holes of the mounting bracket
12. Fasten the screws with a screwdriver

4.4 Cable Connections

4.4.1 Installing the WiN1010 data adapter for WiN5200

The WiN 1010 data adapter is used to power the WiN 5200 and to distribute data.

The WiN1010 data adapter is a combined data and power adapter that interfaces to the customer's Outdoor Unit wireless device. The WiN1010 data adapter unit provides RJ-45 input connectors that include 10/100Base-T transformers for connection to an IEEE802.3 (10/100Base-T) compatible device. The unit receives power from 100V to 240V AC using an IEC-320-C14 industry standard connector.

Important

The power supply AC cord should be 3 wires, 18 AWG minimum, with length less than 4.5 m, safety certified according to national rules

A single output RJ-45 connector provides 10/100 Base-T data and power to the outdoor unit over a Cat 5e cable. This cable serves the bi-directional transfer of data and signaling as well as a power feed to the outdoor equipment.

Note

The Cat5e Ethernet cable is not included. Please refer to "Appendix B – IDU to ODU cable specification" for detailed technical specifications.

The connection schema below illustrates the connections between the devices.

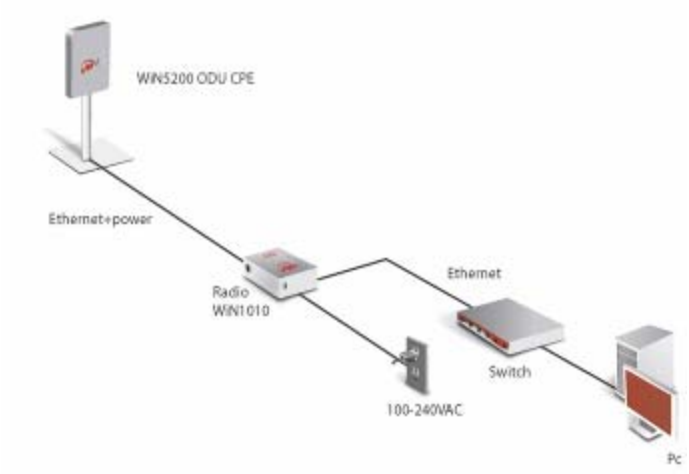


Figure 4-4: WiN5200 Interconnection Schema

Connect the WiN 5200 to WiN 1010 Data Adapter

Connect over a Cat 5e cable the Ethernet port of the WiN5200 to the "ODU IF" port of the WiN 1010.

Note

The Cat5e Ethernet cable is not included. Please refer to "Appendix B – IDU to ODU cable specification" for detailed technical specifications.

Connect the WiN 1010 data adapter to a Switch/Router/PC

Connect over a Cat 5e cable the Ethernet port of the of the WiN1010 data adapter to a 10/100 Base-T port of a Switch/Router/PC. Figure 4-5 illustrates some connection options.

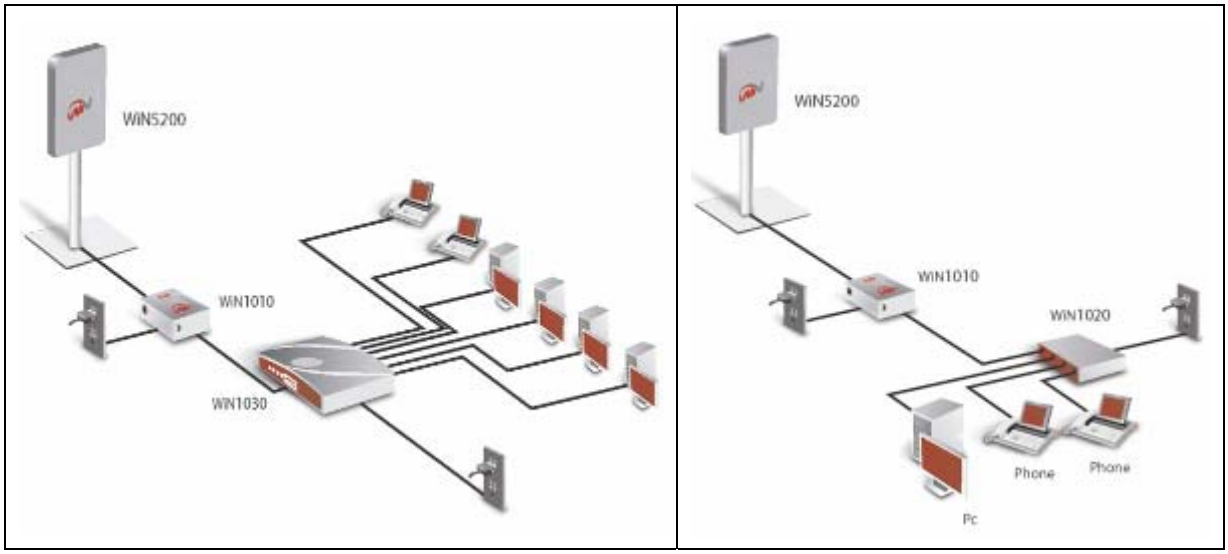


Figure 4-5: WiN1010 Data Adapter Connecting Options

Power Connection

Connect the WiN1010 data adapter to the 110V/220V AC mains using the supplied cable.

Before connecting the WiN1010 data adapter to the main outlet verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.

WiN1010 data adapter LED Indicators

LEDs on the front panel indicate the status of the device.

Figure 4-6: WiN1010 Data Adapter Front Panel

The LEDs are listed by function in the following table.

Table 4-1: WiN1010 data adapter LED Description

WiN1010 data adapter LED Description		
Name	**Color**	**Description**
PWR	Green	Input power is connected
LAN	Green	LAN link/activity display
WLNK	Green	Wireless link/activity display

Table 4-2: ODU I/F port pin-out

ODU I/F - RJ-45	
Pin #	**Description**
1	**ETH Data**
2	**ETH Data**
3	**ETH Data**
4	**+48V**
5	**+48V**
6	**ETH Data**
7	**RTN (-)**
8	**RTN (-)**

Cable Pinout

Ethernet Cable Pinout

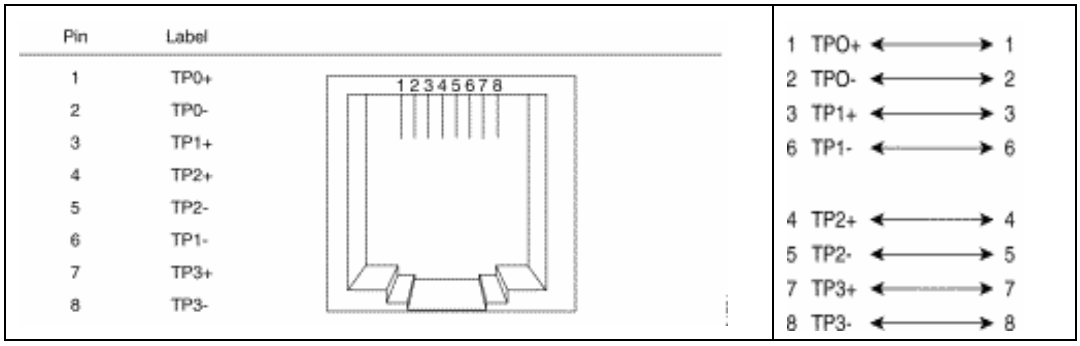


Figure 4-7: Ethernet Cable RJ-45 Pinout

Note

The Cat5e Ethernet cable is not included. Please refer to "Appendix B – IDU to ODU cable specification" for detailed technical specifications.

5

quipment Configuration and Monitoring

5.1 Configuring WiN5200 Basic Parameters

Note

The WiN5200 may be pre-configured in the lab before being sent for installation at the customer's site. In this case, this section can be skipped.

After completing the installation process, the basic parameters must be configured to ensure that the unit operates correctly and can communicate with the base station. Once the basic parameters have been configured, additional parameters can be remotely configured via the wireless link.

1. connect to the IP address `192.168.254.251` with the web browser through the Ethernet port
2. In the Login window, enter username=vendor, password=vendorpass.

Figure 5-1: Login Screen

3. Check the WiN5000/5200 is configured to work in the correct frequency. To do so, choose the "CONFIG" tab and then choose showScanner. Press the "CALL" button. The command lists the channels (frequency and bandwidth pairs) the WiN5000/5200s scan in order to communicate with the base station. The channel values are set at the factory.

Figure 5-2: showScanner screen

4. Use the removeChannelFromScanner command to remove a channel from the scanning procedure. In the id field, enter the ID of the scanned channel (the IDs are shown in the results of the showScanner operation).

Figure 5-3: removeChannelfromScanner screen

5. To add a channel for scanning purposes, select the addChannelToScanner command.

Figure 5-4: addChannelToScanner screen

Enter the bandwidth and the frequency. An ID will be allocated automatically.

Note

The frequency and bandwidth should match the cBST configuration

6. To display physical statistics on the downlink, choose "SS" tab, from the menu on the left hand side of the screen, choose showSsPhyStatDl. Press the "CALL" button. Check the SS RSSI and CINR levels. Hit the "CALL" button to refresh the screen.

Figure 5-5: showSsPhyStatDl screen

Note

This field is only valid when the CPE is synchronized with the cBST.

7. Choose the "SS" tab, from the menu on the left hand side of the screen, choose showSs. Press the "CALL" button. Check if the WiN5000/5200 is in OPERATIONAL status. "OPERATIONAL" status means that the link is up.

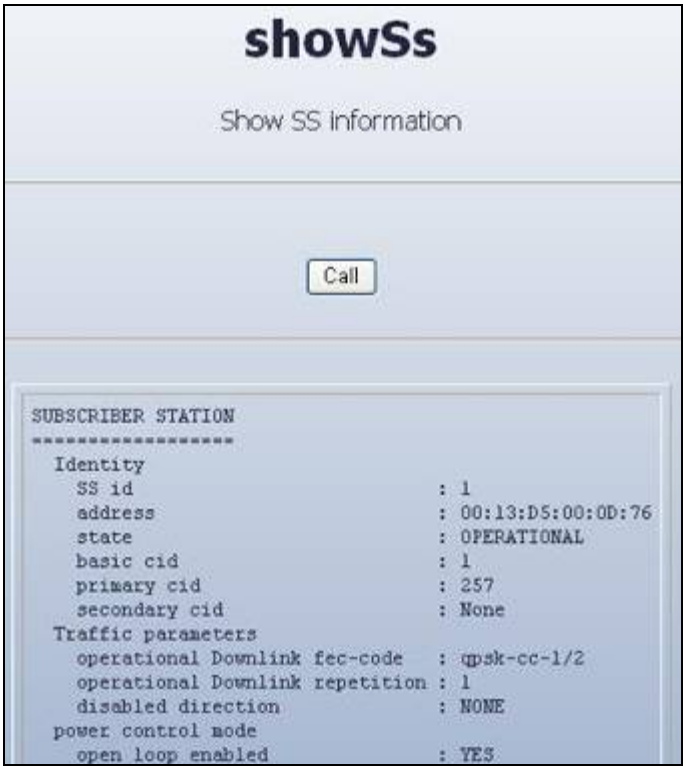


Figure 5-6: showSsPhyStatDl screen

8. Check that all the Service flows are created by using the showSF menu

5.2 Aligning the CPE Antenna

The LINK QUALITY bar display is located on the bottom panel of the outdoor unit. The LED marked WLNK indicates that the wireless link is active, and is lit when the CPE has completed the Network Entry process. There are 8 LEDs that indicate the quality of the received signal. The higher the number of LEDs that are on, the better the quality of the received signal.

This section describes how to align the CPE antenna using the LINK QUALITY bar display.

5.2.1 CPE Antenna Alignment Procedure

- Point the antenna towards the general direction of the Base Station.
- Verify that the power indication of the unit is on.
- Verify that at least one green LED of the LINK QUALITY bar display is on, indicating that the unit is synchronized with the base station. If the CPE is not synchronized with the base station, ensure that all parameters are configured properly. If the CPE is still not synchronized with the base station, improve the quality of the link by changing the direction of the antenna or by placing the CPE at a higher or alternate location.
- Rotate the CPE until the maximum Link Quality reading is achieved. If you encounter prolonged difficulty in achieving the expected link quality, try to improve the reception quality by placing the CPE at a higher point or in an alternate location.

Note

Ensure that the front of the antenna is always facing the Base Station. However, in certain conditions, such as when the line of sight to the Base Station is hampered, better reception may be achieved using a reflected signal. In this case, the antenna is not necessarily directed toward the Base Station

- Secure the CPE firmly to the pole.

Note

In some cases, the antenna may need to be tilted to ensure that the level at which the CPE receives transmissions from the Base Station (and vice versa) is not too high. When all LINK QUALITY LEDS are on. This indicates that the received signal level is too high (saturation). This must be avoided, preferably by up-tilting the antenna. As a rule of thumb, if the CPE is located at a distance of less than 300 meters from the Base Station, it is recommended to up-tilt the antenna by approximately 10° to 15°

Table 3: LINK QUALITY Bar LEDs Functionality

Bar LEDs	SNR
WLNK is On	CPE is connected with and receives services from Base station (Network Entry completed)
One bar LED is On (Least significant)	5dB ≤ SNR < 10dB
Two bar LEDs are On	10dB ≤ SNR < 15dB
Three bar LEDs are On	15dB ≤ SNR < 20dB
Four bar LEDs are On	20dB ≤ SNR < 24dB
Five bar LEDs are On	SNR ≥ 24dB and RSSI < -75dBm

Bar LEDs	SNR
Six bar LEDs are On	SNR ≥ 24dB and RSSI ≥ -75dBm
Seven bar LEDs are On	SNR ≥ 24dB and RSSI ≥ -70dBm
Eight bar LEDs are On	SNR ≥ 24dB and RSSI ≥ -60dBm
Only the 8th LED is On (Most significant)	RSSI ≥ -20dBm (saturation)

Figure 5-7:Example of RSSI Scan behavior

5.2.2 Link Indication

Another function of this LED is to indicate whether or not the SS have a link with the BS.

Blink - the link is down.

Constant light – the link is up.

6

anagement

6.1 General

The CPEs can be monitored and controlled with a standalone PC or through a management system (WiNMS) using the backhaul interface. The monitoring and control capabilities are similar in both cases but the interface may appear different. This section will detail all the monitoring and control capabilities and then will specify which of them are available through each type of interface.

The local PC can connect to the internal WEB server using HTTP.

The CPEs have a standard MIB II and propriety MIB.

Management of the CPE device shall use SNMP.

All levels of management are secured by passwords.

There are no local displays on the CPEs. All the indications will have to be monitored via the management system (WiNMS).

6.2 SW Download/Upgrade

Software can be loaded into the CPE in several ways:

- Using a local PC (connected to the nearby switch)
- Remotely using SNMP (over the backhaul interface)
- Remotely using FTP

The CPE supports a complete rollback option in case the upgrade does not work.

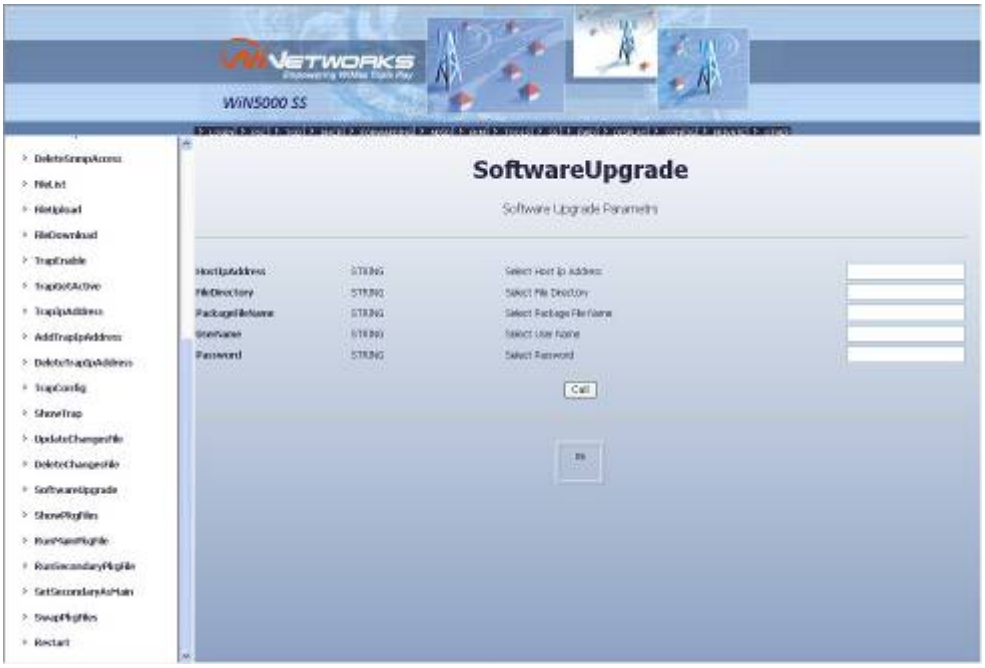


Figure 6-1: SoftwareUpgrade Screen

Fill the FTP server IP address in the HostIpAddress field

Fill the directory in which the new SW files are located in the FileDirectory field

In this directory there should be <filename>.pkg file

Fill in the file name of the .pkg file in the PackageFileName field

Fill in the username and password of the FTP server in the appropriate fields

Press the "call" button

Wait for the upgrade process to complete

6.3 Web-page Management

The monitored and controlled parameters are also available through web-page interface.

Please refer to Section 5 "Equipment Configuration and Monitoring" for basic configuration and monitor screens.

The most common operating commands are listed in the following table. For sake of convenience the commands are listed by tabs of the software.

Table 6-1: List of Commands - Configuration

Tab	Command	Function	Notes
Conf	ShowTxRxparam	Shows the Transmit and Receive parameters	
	showscanner	Shows the scanning list of channels/frequencies	
	addChannelToScanner	Adds a new channel to the scanner	
	removeChannelfromScanner	Removes a channel from the scanning list	
	clearScannerChannel	Resets all channel scanners	
	showMacUl	Shows theMac Uplink configuration	
	showMacDl	Shows the Mac Downlink configuration	
	showRfRx	Shows the Radio Receiver Frequency configuration	
	showRfTx	Shows the Radio Transmitter Frequency configuration	
	showLinkAdaptationDl	Shows the Downlink Adaptation information	

Table 6-2: List of Commands - SS

Tab	Command	Function	Notes
SS	ssPhyStatsDl	Shows the physical status of the device	
	startSs	Starts the 802.16 MAC	
	resetSs	Stops and resets the 802.16 MAC	
	showSs	Shows subscriber station information	

Table 6-3: List of Commands - Tools

Tab	Command	Function	Notes
Tools	showMacAddress	Shows the mac address	
	showMSGProtocol		
	showVersion	Shows the system version	
	showRegisteredMsg	Shows registered Msg	
	showIPAddressTable		
	setIPAddresTable	Set and configure subscriber's IP address	
	showAutorizedManager	Shows a list of authorized managers by IP address	
	showAutorizedManager	Set a list of authorized managers	
	addAutorizedManager	Add authorized manager to the list	
	addAutorizedManager	Delete authorized manager from the list	
	addSnmpAccess	Add SNMP access by IP address	
	DeleteSnmpAccess	Delete SNMP access by IP address	
	Filelist	Shows the list of files	
	FileUpload	Upload files from the computer	
	FileDownload	Download files to the computer	
	Trapenable	Enables traps	
	TarpGetActive	Sends all active traps	
	TrapIpAddress	Sets trap IP address	
	AddTrapIpAddress	Add trap IP address	
	deleteTrapIpAddress	Delete trap IP address	

Tab	Command	Function	Notes
	TrapConfig	Configure a trap	
	showTrap	Shows trap parameters	
	SoftwareUpgrade	Shows software upgrade parameters	
	showPkgFiles	Shows package file indoemation	
	runMainPkfFile	Runs Main Package File	Following the download of a new software package this can be set as the main package. If the last update is not helpful you can set it as secondary package and restart the base station from the previous software version
	runSecondaryPkfFile	Runs Secondary Package File	After reset the station starts from secondary package file
	setSecondaryasMain	Sets Secondary File As Main File	If the last update is not helpful you can set it as secondary package and restart the base station from the previous software version
	swapPkgFiles	Swaps Package Files	Toggles between main and secondary package and saves
	Restart	Restarts Subscriber's Station	

6.4 SNMP Management

There are two MIB types available in the CPE:

- the standard MIB II (RFC 1213)
- the private MIB

Table 6-4 describes the CPE Managed Parameters.

Table 6-4: Subscriber Station Parameters

Parameter	Description	MIB Type	Remarks
Location site + Contact details		MIB II	
Cell ID	Activity (Connected/Disconnected), Speed (10/100/1000), Duplex (Full/Half), IP Address,	Private	
Data Interface Status		MIB II	
Temperature	temperature inside the case	Private	
Software Version	all Modules software's versions	Private	
Uptime	on time from power up	Private	
Number of registered SU		Private	
SU MAC Addresses		Private	
SU Type		Private	
Radio Status	Transmit: On/Off Frequency: configured radio frequency Configured BW/FFT Transmit power	Private	
TX Counter	Number of transmit packets	Private	
RX Counter	Number of receive packets	Private	

Radio and Modem:

Frequency	WiN5125-XX, WiN5225: 2496 MHz to 2690 MHz
	WiN5237: 3650 MHz to 3700 MHz
Radio Access Method	IEEE802.16-2005 (16e OFDMA)
Operation Mode	TDD
Compatibility	WiN52XX-2: Wave 2 Profile (MIMO)
Channel Bandwidth	WiN5125-XX, WiN5225: 5 MHz, 7MHz, 10 MHz
	WiN5137-XX, WiN5237: 5 MHz ,7MHz, 10 MHz
Frequency Resolution	0.25 MHz
Antenna Support	Integral/External
Number of Antennas	2
Antenna Diversity Support	STC/MIMO
Output Power [P1dB]	2W
Output Power (average)	24 dBm +/-1dB maximum
TPC	45dB
FFT/Modulation	1024/512 FFT points;
	QPSK, 16QAM, 64QAM
FEC	Convolution Code and Turbo Code
Dynamic range	RX: -100dBm :-20 dBm
	TX: -20dBm : +24 dBm

Data Communication (Through indoor unit):

Ethernet Standard Compliance	IEEE 802.3 CSMA/CD
Ethernet Port	10/100 Mbps, Half/Full Duplex with Auto Negotiation
VLAN Support	IEEE 802.1Q
Traffic Classification	• IEEE 802.1p • DiffServ (DSCP)
Max User Throughput	DL: 12Mbps, UL: 6Mbps

Ordering Information:

Part Number	WiN52XX-2-02-W
XX – Frequency range	See frequency table for details

Indoor Unit (ETH) Compatibility:

WiN1010	Data Adapter

Configuration and Management:

Local Management	• Telnet • SNMPv2 • Web Browser
Remote Management	SNMPv2 over wireless via the base station
SNMP Agent	SNMP ver 2 client: MIB II (RFC 1213), Private Win-Max MIBs
Authentication	EAP-TTLS:
	Device: X509 digital certificate
	User: MS-CHAP
Software Upgrade	FTP
Remote Configuration	FTP

Mechanical, Electrical and Environmental:

Dimensions (w/o the antenna) [H, W, D]	224 x 92 x 61 mm
Weight	1.5 kg
Power Source	48VDC from the indoor unit over the indoor-outdoor cable
Power Consumption	17W maximum
Operating Temperature	-40°C to +55°C
Operating Humidity	5%-95% non condensing, Weather protected

Standards Compliance:

EMC	FCC part 15, subpart B, class B
	ETSI EN 301489-1/4
Safety	TUV-UL 60950-1
	EN 60950-1
Radio	FCC Part27
	ETSI EN 302 326-1/2/3
Environmental	ETS 300 019
Enclosure	Type 3R (IP66)

ppendix B – IDU to ODU Cable Specifications

Special 4x2x24 AWG FTP Cat. 5e Outdoor Double Jacket Data Cable UL (1581 VW 1)

Applications:	Outdoor installations, Fixed or portable installations, Digital distribution frames in transmission stations, Outdoor installations in harsh environments
General Construction:	Custom made cable designed specially for wireless systems, meeting the requirements of Cat. 5e per ANSI/TIA/EIA-568-B.2 and IEC 61156-5. The cable contains 4 twisted pairs, cabled, foil-tape shielded and jacketed with two special black UV resistant, flame retardant PVC compounds for direct outdoor use in harsh electrical environments. The diameter of the inner core complies with RJ45 connecting hardware allowing direct connection to equipment without patch cords.
Conductor Size:	0.52 mm
Outer Jacket Material:	UV resistant FR-PVC
Outer Diameter:	7.9 mm nom.
Weight:	68.0 kg/km

Design & Materials

Conductor Material:	Bare Copper
Conductor Size:	24 AWG
Insulation Material:	Solid PO
Insulation O.D.:	1.07 mm
Color code:	Per TIA/EIA 568-B
Overall Foil Shield:	Yes
Overall Shield Material:	Aluminum/Polyester Foil
Overall Foil Design:	100% Coverage
Overall Drain-wire Material:	Tinned Copper
Overall Drain-wire size:	24 AWG
Overall Drain-wire Construction:	Stranded
Inner Jacket Material:	UV resistant FR-PVC
Inner Jacket Diameter:	6.1 mm
Total number of wires:	8

Standards

Flamability Rating:	IEC 60332, UL 1581 VW-1
Standards:	IEC 61156, TIA/EIA-568

Performance

Frequency Range:	1 - 100 MHz
Impedance:	100 Ω
DC Resistance:	93 Ω/km nom.
Max. DC Resistance :	95 Ω/km@20°C
Capacitance Unbalance:	1.6 pF/m max.
Velocity of Propagation:	68 % nom.
Propagation Delay Skew:	35 ns/100m max.
Dielectric Strength:	700 V/minute
Dielectric Strength to Shield:	700 V/minute
Min. Bend Radius:	70 mm
Max. Operating Temperature:	+70 °C
Min. Operating Temperature:	-40 °C

ist of Acronyms

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
ALG	Application-Level Gateway
AMC	Adaptive Modulation and Coding
API	Application Programming Interface
ARPU	Average Revenue Per Unit
ASN	Access Service Network
ASP	Application Service Provider
ATPC	Automatic Transmit Power Control
BE	Best Effort
BPSK	Binary Phase Shift Keying
BST	Base Station
BWA	Broadband Wireless Access
CAPEX	Capital Expenditure
CBST	Compact Base Station
CPE	Customer Premise Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Multiplexer
DVB	Digital Video Broadcast
EAP	Extensible Authentication Protocol
ErtPS	Extended Real-Time Polling Service

FCAPS	Functionality Configuration Accountability Performance Security
FFT	Fast Fourier Transfer
FTP	File Transfer Protocol
FUSC	Fully Used Sub-Channelization
FXS	Foreign Exchange Subscriber
GW	Gateway
HA	Home Agent
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IDU	Indoor Units
IEEE	Institute of Electronic and Eclectic Engineers
IGMP	Internet Group Multicast Protocol
IMS	IP Multimedia System
IOS	Internetwork Operating System
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
LOS	Line-of-sight
MAC	Media Access Control
MAI	Multiple Access Interference
MAN	Metropolitan Area Network
MGCP	Media Gateway Control Protocol
MIMO	Multiple-Input, Multiple-Output
MIP	Mobile IP
MOS4	Mean Opinion Score (voice quality 1-5)
MOS5	Mean Opinion Score (voice quality 1-5)

MSG	Multi-Service Gateways
MTU	Maximum Transmission Unit
MTU	Multiple Tenant Unit
NAP	Network Access Provider
NAPT	Network Address Port Translation
NEBS	Network Equipment Building System
NMS	Network Management System
NLOS	Non-line-of-sight
nrtPS	Non-Real Time Polling Service
NSP	Network Service Provider
NVoD	Near Video on Demand
NWG	Network Working Group
OAM	Operations and Maintenance
ODU	Outdoor Units
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal frequency division multiple access
OPEX	Operational Expenditure
P-CSCF	Proxy - Call Session Control Function
PDA	Personal Digital Assistant
PDF	Portable File Format
PMIP	Proxy Media IP
POP	Point of Presence
POP3	Post Office Protocol 3
POTS	Plain Old Telephony System
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Phase Shift Keying

PSTN	Public Switched Telephone Network
PUSC	Partially used sub-channelization
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RC	Return Channel
RF	Radio Frequency
RG	Residential Gateway
RIP	Routing Information Protocol
ROI	Return of Investment
rtPS	Real-Time Polling Service
SF	Service Flow
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
S-OFDMA	Scalable Orthogonal frequency division multiple access
SOHO	Small Office/Home Office
SS	Subscribers
STB	Set Top Box
STC	Space-time coding
SU	Subscriber Unit
TCP	Transmission Control Protocol
TDD	Test Driven Design
TFTP	Trivial File Transfer Protocol
TMN	Telecommunication Management Sysytem
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service

URL	Universal Resource Locator
USB	Universal Serial Bus
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLL	Wireless Local Loop
WMAN	Wireless Metropolitan Area Networks